Declassified in Part - Sanitized Copy Approved for Release 2013/03/18 : CIA-RDP87B00342R001002120016-5

[redacted]

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755

Executive Registry
85- 2400

Serial: N1078-85
30 May 1985

WKO 3 June

MEMORANDUM FOR THE ASSISTANT SECRETARY OF DEFENSE C3I

SUBJECT: Director of Central Intelligence Memorandum NFIC-9.11/1 dated 22 Jan 85 - INFORMATION MEMORANDUM

The DoD Computer Security Center has reviewed the document "UNIFORM SAFEGUARDS FOR PROTECTION OF 'CRITICAL SYSTEMS' PROCESSING INTELLIGENCE INFORMATION". We thank you for the opportunity to review this document and to provide what we believe are important comments. Specific comments are given in the enclosure. General comments follow:

This document has several flaws, chief of which is the allowing of multilevel mode operation without secure systems. The document states that it is not necessary to implement security-related software in the operating system. Therefore, the highest class of system that would be produced using this document would be a B1, according to the Department of Defense Trusted Computer System Evaluation Criteria (hereafter referred to as the Criteria). Further, this document implies that it is permissible under certain circumstances to operate the system in multilevel mode with users possessing a wide range of clearances. Because the maximum achievable evaluation class is a B1, most critical systems should NEVER be allowed to operate in multilevel (or compartmented) mode with users possessing a wide range of clearances.

If this document were to be implemented as written, it would result in the Intelligence Community having a false sense of security about its critical systems. This could then result in a lessening of the effort currently underway to encourage development of truly secure systems.

This document contradicts much of the guidance that the Center has promulgated in the Criteria. It quotes some passages directly from the Criteria without ever citing the Criteria. In so doing, it distorts the intent of the Criteria in some places. The SAFEGUARDS document should be changed to be consistent with the Criteria.

THIS DOCUMENT MAY BE
DECLASSIFIED UPON
REMOVAL OF ENCLOSURE

[redacted]

5-327

Declassified in Part - Sanitized Copy Approved for Release 2013/03/18 : CIA-RDP87B00342R001002120016-5

Declassified in Part - Sanitized Copy Approved for Release 2013/03/18 : CIA-RDP87B00342R001002120016-5

Parts of this SAFEGUARDS document are very misleading. For the past three years, the terms "mandatory access control" and "discretionary access control" have consistently been interpreted to mean that access decisions are made by the Trusted Computing Base (TCB) of the system. This document uses the terms to indicate that some access decisions are made through environmental and administrative mechanisms. If the document is going to discuss both hardware/software mechanisms and environmental/administrative mechanisms, it must make this distinction clear from the beginning. One suggestion would be to use different terminology for hardware/software controls than is used for environmental/administrative controls.

As written, this document implies that no existing "Critical System" can ever be enhanced above a B1 level. (For example, the topic of covert channels, which first appears in the Criteria at the B2 level, is not addressed at all.) The Center agrees with this assessment, and believes that this point should be explicitly stated. Further, the Center's current guidance indicates that D systems may only be used in dedicated mode, C systems may only be used in system high or dedicated mode, and B1 systems may only be used in a few multilevel and compartmented environments, along with system high and dedicated mode. Therefore, there is an implicit mapping between the levels suggested in the SAFEGUARDS document and the Criteria evaluation classes. The Center believes that this mapping should be stated explicitly in the document.

In summary, the Center believes that: (1) the SAFEGUARDS document has major flaws that must be addressed before it is issued; (2) this document should be changed to be consistent with the Criteria; and (3) if implemented as currently written, this document would allow multilevel operation of unsecure systems.

25X1

for
Computer Security

Encl:
a/s

Declassified in Part - Sanitized Copy Approved for Release 2013/03/18 : CIA-RDP87B00342R001002120016-5

Declassified in Part - Sanitized Copy Approved for Release 2013/03/18 : CIA-RDP87B00342R001002120016-5

COMMENTS ON THE "UNIFORM SAFEGUARDS FOR PROTECTION OF 'CRITICAL SYSTEMS' PROCESSING INTELLIGENCE INFORMATION"

1. (U) General comment: Many of the requirements in the SAFEGUARDS document are introduced at implicitly much lower levels of "evaluation classes" than they are in the Criteria. The usefulness of requiring the safeguards for the lower level system is questionable, since they are generally expensive and do not result in much gain in security for lower level systems, due to the general system architecture. Among these requirements are: trusted distribution, trusted path, and configuration management.

2. (U) Top of p. 2: Why is "labeling" distinct from "access controls"? The Center's viewpoint is that labels are used as a mechanism for performing access control. Therefore, labeling of data without corresponding access controls is meaningless and is simply a waste of effort.

3. (U) Page 3, last para.: While Terminal Identification is required by the Criteria, the current interpretation of this requirement is that it is the communication port to which the terminal is connected which must be identified. This is because of the fact that Terminal Identification is difficult to implement and easy to spoof unless a terminal can be physically hardwired to one of the system's communication ports.

4. (U) Page 4, second para.: What does it mean for a function to have "Control Labels"? What really happens is that an object which when executed performs some function has a label indicating the sensitivity level of the subject on whose behalf it is processing. This point should be stated explicitly.

5. (C) Page 6, last sentence: Many of the security-related automated controls <u>can</u> be implemented in the operating system now. It has been shown that most operating systems are extensible to the B1 level, without needing to be redesigned. The fact that an A1 system cannot be developed overnight does not mean, as this sentence seems to imply, that application-level security features are the best that can be provided.

6. (U) Page 10, table 1: This table is very misleading. In general, this document is mixing apples and oranges in that it talks about safeguards in general, without regard to whether they are implemented by hardware/software mechanisms or by personnel, physical, and procedural mechanisms. The specification of the document should be as follows:

Dedicated mode systems: for systems operating in dedicated mode, all safeguards are done by physical, personnel, and procedural mechanisms. Since all users of the system are by definition cleared for and possess need-to-know for all data on the system, there is no need for any hardware/software safeguards.

Declassified in Part - Sanitized Copy Approved for Release 2013/03/18 : CIA-RDP87B00342R001002120016-5

Declassified in Part - Sanitized Copy Approved for Release 2013/03/18 : CIA-RDP87B00342R001002120016-5

System high systems: all users of systems operating in system high mode are cleared for all data on the system, but may not have a need-to-know for all of it. Therefore, the hardware/software of the computer system must provide discretionary controls and audit trails. Since all mandatory access controls are performed by procedural, personnel, and physical security mechanisms, it is not necessary for the system to support mandatory access controls or labeling.

Compartmented and multilevel systems: since some users of the system are not formally cleared (or authorized) for some of the data being processed by the system, the system must support both mandatory and discretionary controls.

7. (U) Page 11, Table 2: The row labeled "User need-to-know" is very misleading. For the system to be operating in a secure manner, the user must have a need-to-know for all types of information that he is allowed to access. If a user is allowed to access any information for which he does not possess a need-to-know, it is a violation of discretionary security policy. This should be clearly indicated in this table, or else this row should be deleted from this table.

8. (U) Page 11, Table 2: The Multilevel column indicates that the range of clearances for system users can be anywhere from uncleared to Top Secret SBI clearance. On page 9, in the paragraph defining Multilevel mode, it indicates that the clearances of users may range from Secret to Top Secret SBI. This contradiction needs to be resolved.

9. (C) Page 11, Table 2: Going back to the comment about it not being necessary to implement security-related software in the operating system, this table implies that it is permissible under certain circumstances to operate the system in multilevel mode with users possessing a wide range of clearances. Since the maximum level of system that can be developed under this document is a B1, most critical systems should NEVER be allowed to operate in multilevel (or compartmented) mode with users possessing a wide range of clearances.

10. (C) Page 17, First para.: Since all users are cleared for all data being processed on system high systems, mandatory access controls are implemented with personnel, physical, and procedural security mechanisms. Even though current DCI policy requires labeling of data on a system operating in system high mode, the Information System Security Officer should be aware that, without accompanying mandatory access controls, labels cannot be trusted to be an accurate reflection of the information's true sensitivity. Therefore, users should treat all information as being classified at the system high mark until it has been manually reviewed for classification.

11. (U) General comment: Replace "security related software" with "Trusted Computing Base" or "TCB". This will make the document consistent in terminology with the Criteria. (U)

Declassified in Part - Sanitized Copy Approved for Release 2013/03/18 : CIA-RDP87B00342R001002120016-5

Declassified in Part - Sanitized Copy Approved for Release 2013/03/18 : CIA-RDP87B00342R001002120016-5

12. (U) Page 19, last para.: Trusted Distribution occurs only at the A1 level of the Criteria. Since none of the systems mentioned in the document can possibly be enhanced to beyond the B1 level, this requirement is expensive and results in little security gain. (See comment #1.)

13. (U) Page 20, last para.: This states that Test Documentation is a requirement for systems operating in System High mode. This is in direct contradiction to Table 1, page 10.

14. (U) Page 25, third para.: The requirement for a trusted path occurs at the B2 level in the Criteria. Below this level, the TCB is sufficiently weak that a trusted path between the user and the TCB is not worth the cost of implementing it.

15. (U) Page 33, first para.: Replace the word "contains" with the word "dominates".

16. (U) Page 35, first para.: The last sentence doesn't make sense: "No design flaws and implementation flaws found during texting shall be corrected and retested."?

17. (U) Page 40, third para.: If a network is operating in Dedicated mode or System high mode, it is assumed that there may be no hardware/software mandatory access controls. Therefore, once again an explicit label may not accurately reflect the true sensitivity of the data. In this case, the sensitivity of the data is equal to the level of the network. This point should be stated explicitly.

18. (U) Page 40, last para.: In many cases, the size of a network and the size of the user population preclude the network from being able to individually identify each user. If it is indeed feasible, it may be required that the network identify the individual user in the network action log; however, this should not be a generic requirement.

19. (C) Page 41, paras. on Routine Security Report and Special Security Report: What is the difference between a "security incident which has potential network security implications" and a "system abnormality that provides reason to suspect a covert violation of the security integrity of the 'critical system' or network"? It seems that the first necessarily implies the second.

20, (U) Page 44, def. of Subject Security Level: A subject may have read only access to a variety of objects at a variety of security levels. Therefore, the Subject Security Level is equal to the security level of the objects to which it has both read and write access. If a subject has read only access ONLY, the subject security level is equal to the highest security level of the objects to which it has read only access.

Declassified in Part - Sanitized Copy Approved for Release 2013/03/18 : CIA-RDP87B00342R001002120016-5